UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,851	05/22/2001	Ralph S. Hoefelmeyer	COS 00 017	8371

25537 7590 01/27/2005

MCI, INC
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW, 10TH FLOOR
WASHINGTON, DC 20036

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/862,851	HOEFELMEYER ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *20 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-32 are pending in the Application.

Claims 1,8,9,16-23, 25-30 are currently amended.

In view of Applicant's amendment and arguments a new ground (s) of rejection is presented in this office action, therefore, response to the applicant's arguments is moot.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5-7, 9, 13-15, 17-20, 22-23 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Ji et al. (US Pat. No. 5,623,600, hereinafter "Ji") and further in view of Xu, US Patent Pub. No. 2002/0032766.

As per claims 1 and 9, Ji teaches a method /system for malicious code detection (abstract), comprising:

a front-end processor, coupled to a scanning computer system, configured for receiving a flow of content from an external network and distributing a copy of the flow the scanning computer system for scanning [col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40], and

a detection management system, coupled to the scanning computer system, configured for employing a countermeasure on the flow if the scanning computer system generates the alarm [col. 11, lines 3-40].

Ji fails to teach "a plurality of scanning computer systems" and distributing " a common copy of the flow to each of the scanning computer systems in parallel for scanning".

However, the examiner asserts that the use of multiple virus scanning devices scanning a common copy of the flow in parallel is well known in the art.

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems for scanning a common copy of the flow in parallel because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

As per claim 5, claims 13 and 31-32, Ji fails to teach scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code.

However, the examiner asserts that the use of multiple virus scanning devices with different detection software and with different coverage of malicious code is well known in the art.

It would have been obvious to one of ordinary skill in the art to modify the Ji's scanner to incorporate virus scanning software differ in their capabilities as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228.

As per claims 6 and 14, Ji teaches the system/method according to claims 1 and 9, wherein the flow includes at least one of a hypertext markup file and a transferred file [col. 5, lines 28-38].

As per claims 7 and 15, Ji teaches the method/system according to claims 1 an 9, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow,

and informing the recipient of the flow of the malicious code [col. 11, lines 3-40]. That is, Ji's proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of Ji suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined).

Claim 17 is an apparatus (front end system) reciting limitations of claims 1 and 6. Claim 17 is rejected for the same reasons stated in the statement of rejection of claims 1 and 6 above.

Claim 18 is a method claim reciting limitations of claims 1 and 6. Claim 17 is rejected for the same reasons stated in the statement of rejection of claims 1 and 6 above.

Claim 19 recites a storage medium having instructions to execute the method of claim 18, therefore the same rejection applies.

Claim 20 is an apparatus claim reciting limitations of claims 1 and 6. Claim 20 is rejected for the same reasons provided in the statement of rejections of claims 1 and 6 above.

Claims 22-23 recites a detection management system with features recited in claims 1, 6 and 7. Claims 22-23 are rejected for the same reasons stated in the statement of rejections of claims 1, 6 and 7 above.

Claims 2-4, 10-12, 8, 16 and 24-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Ji et al and Xu as applied to claims 1 and 9 above and further in view of Wells (US. Pat. No. 6,338,141).

As per claims 2-4, 10-12, Ji as modified fails to teach a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer system,

a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat,

wherein the detection management system id further configured for causing the signatures stored at the remote detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses, are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Ji to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, Wells, col. 2, lines 22-46.

As per claims 8 and 16, Ji teaches a system/method for malicious code detection, comprising:

a front-end processor, coupled to the scanning computer systems, configured for receiving a flow of content from an external network and distributing a common copy of the flow to each of the scanning computer systems in parallel for scanning, said flow including at least one of a hypertext markup file and a transferred file [col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40]; and

employing a countermeasure on the flow if at least one of the scanning computer systems generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code and generating an alarm when the content contains malicious code [col. 11, lines 3-40];

Ji fails to teach a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for scanning content for malicious code;

However, the examiner asserts that the use of multiple virus scanning devices in parallel with different detection software and with different coverage of malicious code is well known in the art.

It would have been obvious to one of ordinary skill in the art to modify Ji 's scanning system to incorporate a plurality of virus scanning systems differ in their capabilities be used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).

Ji-Xu combination fails to teach a detection management system, coupled to the scanning computer systems, configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computer systems generates an alarm on the piece of malicious code; and

causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses, are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Ji to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, Wells, col.2, lines 22-46.

Claim 24 is an apparatus reciting limitations of claims 1, 2 and 4. Claim 24 is rejected as such.

Claims 25-27 recite limitations (broader in scope) of apparatus claims 1, 2, 4, 6 and 7. Claims 25-27 are rejected for the same reasons provided in the statement of rejections of claims 1,2,4,6 and 7 above.

In regards to claims 28-30, the claims limitations recite a storage medium having computer programs to execute the steps of 1- 4, 6 and 7, therefore the same rejection applies.

Conclusion

Prior arts made of record, not relied upon:

US Pat. Pub. No. 2002/0069356 is directed to a networking system with an integrated security gateway for integrating virtual private networking, firewall, and network monitoring functions. A duplicate of a received packet is provided to a network monitoring system connected thereto or included therein so as to detect all kind of intrusions and attacks to a virtual private network and the integrated security gateway itself. And, by implementing a variety of functions and services in the network monitoring system, the network system of the invention enjoys almost complete security.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100